(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 862 104 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.09.1998 Bulletin 1998/36

(51) Int. Cl.[6]: G06F 1/00

(21) Application number: 98103380.6

(22) Date of filing: 26.02.1998

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 28.02.1997 JP 46038/97
16.12.1997 JP 363335/97

(71) Applicant:
Casio Computer Co., Ltd.
Shibuya-ku, Tokyo 151-8543 (JP)

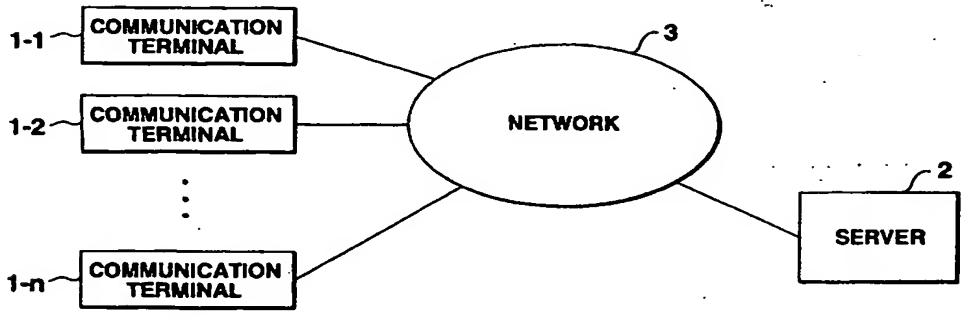
(72) Inventors:
- Moriya, Koji,
c/o Casio Computer Co., Ltd.
Hamura-shi, Tokyo 205-8555 (JP)
- Morikawa, Shigenori,
c/o Casio Computer Co., Ltd.
Hamura-shi, Tokyo 205-8555 (JP)

(74) Representative:
Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) Authentication system using network

(57) A communication terminal (1) stores an assigned telephone number and a number unique to the terminal. When on-line registration is to be conducted with respect to a server (2), a registration screen is automatically created. On the registration screen, predetermined information is already described as entry matters required for registration by using the above described numbers. By inputting a password to this screen, the user can complete on-line registration simply. When the server (2) provides service, the server requests the user to input the user name and the password. As for the communication terminal (1), the server has beforehand the telephone number, information unique to the terminal, and the like in the database. In response to a communication request from the communication terminal (1), the server (2) conducts authentication by using the telephone number as the user name and the terminal number as the password.

FIG.1



EP 0 862 104 A2

Description

The present invention relates to a system for registering a terminal device into a server on a network and authenticating a terminal device. In particular, the present invention relates to a system for simply conducting registration and authentication of a terminal device having a telephone function.

In recent years, it has become possible to connect an information processing terminal such as a personal computer or a portable terminal to a communication network such as a commercial network or the Internet and make various kinds of service such as electronic mail transmission and reception easily usable. Furthermore, in recent years, portable information processing terminals incorporating a telephone function are also becoming sold. Ordinary persons who are not familiar with personal computers have increased opportunities to use networks.

For connecting an information processing terminal to a communication network, it is necessary to conduct a registration (or subscribing) procedure for a commercial network company in the case of a commercial network, and for an Internet connection company called provider in the case of the Internet.

For conducting registration for a provider, a procedure of filling in a registration blank followed by mailing it, or of inputting necessary matters by means of on-line sign up is required. This procedure is a very troublesome work for a person who is not familiar with personal computers. Even after subscribing, it is necessary for connection to the network to conduct an authentication check between a terminal (or an individual) and a server providing service on the network. Each time connection to the network is conducted, the user needs to accurately input the user's name (or ID) and a password. In many cases, the user ID and password are meaningless character strings. Therefore, there is also inconvenience caused when the user has forgotten the user ID and password.

An object of the present invention is to make it possible to reduce the required entry matters in the on-line registration.

Another object of the present invention is to facilitate also the authentication conducted when connecting a terminal device to a server.

For achieving these objects, according to a first aspect of the present invention, there is provided a communication processing device conducting data communication with a communication service providing device connected via a communication circuit, the communication processing device comprising:

a first memory for storing a unique information assigned beforehand;
input guide means for causing a user to input a password for registering in the communication service providing device in response to specification of registration processing execution of its own communication processing device with respect to the communication service providing device; and
transmission means for transmitting the password inputted by the user according to the input guide means and the unique information stored in the first memory to the communication providing device,
wherein registration of its own communication processing device with respect to the communication service providing device is conducted by using the unique information and password.

According to a second aspect of the present invention, there is provided an authentication system in a network system including a server and terminal devices, the server authenticating a terminal device based on data transmitted by the terminal device, the server providing an authenticated terminal device with service,

the server comprising:

terminal information storing means for storing terminal information including a terminal code and a telephone number belonging to each of the terminal devices;
receiving means for receiving a connection request and terminal information of a terminal device transmitted from the terminal devices; and
authentication means for collating the terminal information transmitted from the terminal device with the terminal information stored in the terminal information storing means, and for authenticating the terminal device and permitting the connection when substantial coincidence is found, and

each of the terminal devices comprising:
storing means for storing a terminal code of the terminal device and a telephone number assigned to the terminal device as terminal information; and
transmitting means for transmitting a connection request and the terminal information stored in the storing means to the server.

According to a third aspect of the present invention, there is provided a terminal device having a telephone function, the terminal device being connected to a server via a network in order to be given information providing service, the terminal device comprising:

storing means for storing information unique to the terminal device and a telephone number assigned to the terminal device; and
transmission means for transmitting the information unique to the terminal device and the telephone number stored in the storing means to the server as authentication data when the terminal device is

connected to the server.

According to a fourth aspect of the present invention, there is provided a server for providing terminal devices having a telephone function connected to the server via a public telephone circuit with communication service, the server comprising:

terminal information storing means for storing terminal information including at least one of information unique to a terminal and a telephone number of each of the terminal devices;
receiving means for receiving the information unique to a terminal and/or the telephone number of the terminal device when the terminal device has requested connection; and
authentication means for collating the information unique to the terminal and/or the telephone number received by the receiving means with the terminal information stored in the terminal information storing means, and for determining whether the terminal device should be connected to the server.

This invention can be more fully understood from the following detailed description when taken in conjunction with the accompanying drawings, in which:

FIG. 1 is a diagram showing the configuration of a first embodiment of a network system according to the present invention;
FIG. 2 is a diagram showing the configuration of a communication terminal according to the present invention;
FIG. 3 is a diagram showing an example of terminal information stored in a memory of a communication terminal;
FIG. 4 is a configuration diagram of a server according to the present invention;
FIGS. 5A through 5C are diagrams showing a series of operation flow charts of a terminal device to which a communication processor of a first embodiment according to the present invention has been applied;
FIG. 6 is a flow chart of a service provider side;
FIG. 7A is a diagram showing a telephone screen at the time when registration is not registered yet, FIG. 7B is a diagram showing a service subscribing screen displayed when provider icons are manipulated on the telephone screen, FIG. 7C is a diagram showing the telephone screen displayed after registration, and FIG. 7D is a diagram showing a service menu screen displayed when manipulating provider icons after registration;
FIG. 8 is a diagram showing an example of terminal information stored in a database;
FIG. 9 is a flow chart illustrating the operation of an authentication method concerning a second embodiment according to the present invention;
FIG. 10 is a diagram showing another example of terminal information stored in the database; and
FIG. 11 is a diagram showing another example of terminal information stored in the database.

The configuration of a network system of an embodiment according to the present invention is shown in FIG. 1.

As illustrated, this network system comprises a plurality of communication terminals 1-1 through 1-n, a server 2 provided in a service provider, and a network 3. Via the network 3, the communication terminals 1-1 through 1-n are connected to the server 2. The network 3 is public circuit such as telephone circuit.

Each of the communication terminals 1-1 through 1-n is a computer connected to a modem, a terminal adapter, or the like, or a portable electronic device such as a PDA (Personal Data Assistance).

FIG. 2 shows the configuration of a PDA having a telephone function. Hereafter, this device will be described as a terminal device 1 representing the communication terminals 1-1 through 1-n.

The terminal device 1 comprises a CPU 11, a RAM 12, a ROM 13, a display unit 14, an input unit 15, a flash ROM 16, a radio communication unit 17, and a sound processing unit 18. These components are interconnected via a bus 19.

The CPU 11 controls the components included in the terminal device 1.

The RAM 12 comprises a semiconductor memory or the like, and is used a main storage area of the CPU 11.

The ROM 13 comprises a mask ROM or the like, and stores an operation program and the like of the terminal device 1. The medium storing the operation program of the terminal device 1 may be a magnetic or optical storage medium. The storage medium is installed fixedly, or mounted so as to be freely attachable and detachable.

The display unit 14 comprises liquid crystal display elements or the like, and displays a result of processing conducted by the CPU 11 and data transmitted from the server 2.

The input unit 15 has a keyboard, various buttons, and the like for inputting a command, an electronic mail, or the like to be transmitted to the server 2.

The flash ROM 16 is an electrically rewritable nonvolatile memory. In this flash ROM 16, a telephone number of the terminal device 1 fixed when the terminal device 1 is sold (or when a contract is made), a terminal number (terminal ID) fixed at the time of manufacturing, and a device kind code are stored as information unique to the terminal as shown in FIG. 3. The terminal number comprises a country code, a manufacturing maker code, and a manufacturing serial number, and differs from device to device.

The terminal number and the device kind code are written into the flash ROM 16 in its manufacturing fac-

tory at the timing of shipping or the like. The telephone number is written into the flash ROM 16 in a store at the time of contract.

The flash ROM 16 is adapted to store the telephone number of the service provider and a registration completion flag in order to be given the network service. As occasion demands, a password may be stored in the flash ROM 16.

As for the flash ROM 16, its configuration is not restricted so long as it is a nonvolatile memory of such a type that a terminal number and a telephone number can be written therein at the time of shipping and selling. The flash ROM 16 may be replaced by a backed up RAM or the like.

The radio communication unit 17 is connected to a network 3 including radio public circuit, and transmits/receives data, sound and the like to/from the other party.

The sound processing unit 18 has a microphone, a speaker, or the like. The sound processing unit 18 reproduces a received sound, and emits the reproduced sound. The sound processing unit 18 also modulates a sound picked up by the microphone and transmits the modulated sound.

As shown in FIG. 4, the server 2 comprises a CPU 21, a RAM 22, a storage unit 23, a database 24, and a communication unit 25. These components are interconnected via a bus 26.

The CPU 21 controls the components of the server 2, and reads out and executes programs stored in the storage unit 23.

The RAM 22 comprises a semiconductor memory or the like, and it is used as a main storage area for the CPU 21.

The storage unit 23 comprises a magnetic disk device or the like, and it stores operation programs such as application programs and transmission/reception program.

The database 24 has a database 24-1 concerning telephone subscribers, a database 24-2 concerning users who contracted so as to be given service provided by the server 2, and various other databases required for providing service.

The telephone subscriber information includes data such as a telephone number, a device kind code, a terminal number (ID), a subscriber name, and a subscriber address. This information is obtained by the provider with the cooperation of a telephone company.

The user information is data of a user given the service by the provider, such as a user name (which is a broad concept including a user ID), password, address, and billing information.

The communication unit 25 has a circuit terminal device, such as a modem, connected to the network 3, and transmits/receives data to/from the communication terminals 1-1 through 1-n.

Operation conducted in such configuration will now be described.

FIGS. 5A through 5C are a series of flow charts showing the operation of the terminal device 1.

First of all, in the case where, for example, power is turned on and a telephone screen is displayed as an initial screen, number buttons 36A, a telephone icon 36B, an electronic mail icon 36C, and so on are displayed on the display unit 14 as shown in FIG. 7A (step S10). It is here determined whether the provider registration completion flag is stored beforehand in the flash ROM 16 (step S12). If there is no provider registration completion flag, a nonregistration icon 36D is displayed on the telephone screen as a provider icon (step S14).

Here, icon manipulation is waited (step S16). If icon manipulation using the input unit 15 is conducted, it is determined whether a provider icon (nonregistration icon 36D in this case) has been manipulated (step S18). If a different icon has been manipulated, processing corresponding to that manipulation icon is conducted. Since the processing has no relation to the principal point of the present invention, description thereof will be omitted.

When the provider icon is judged to have been manipulated (step S18), it is determined whether the provider registration completion flag is stored beforehand in the flash ROM 16 (step S20). If there is no provider registration completion flag, then a service subscribing screen as shown in FIG. 7B is displayed on the display unit 14 (step S22), and the ID and registered telephone number are read out from the flash ROM 16 (step S24) and displayed on the service subscribing screen (step S26). A message requesting password inputting is displayed (step S28).

In response to this, the user inputs a desired password (step S30), and manipulates a registration button 36E (step S32). As a result, a specific provider is called according to the telephone number of the service provider stored in the flash ROM 16, and a circuit connection request (registration request in this case) is transmitted (step S34). The device kind code, ID, inputted password, and telephone number of the terminal device 1 are transmitted (step S36), and a response is waited (step S38). The inputted password may be written into a predetermined area of the flash ROM, and at the next time on the server access is requested, this stored password may be transmitted in order to omit the user's input manipulation.

FIG. 6 is a flow chart showing the operation of the server 2 located on the side of the service provider.

Upon receiving the circuit connection request, it is first determined whether the circuit connection request is a registration request (step S100). If the circuit connection request is a registration request, the device kind code, ID, password, and telephone number are received (step S102). And the database 24-1 of telephone subscriber information stored beforehand is referred to, and a check is executed to determine whether the validly registered telephone number and ID have been transmitted (step S104). If the result is permissible (step

S106), then authentication data concerning the user which has been connected for the first time in order to conduct registration is created on the basis of the password and the like of the received data and the data of the telephone subscriber database, and registered into the user database 24-2 (step S108), and a permission response is transmitted (step S110).

On the other hand, if the result of the validity check is impermissible (step S106), then nonpermission response is transmitted (step S112).

Upon receiving a response from the service provider (step S38), the terminal device 1 determines whether the response is a permission response (step S40). If the response is a permission response, then the registration completion flag is set in the flash ROM 16 (step S42), a registration completion message is displayed for a fixed time (step S44), and then a telephone screen is displayed as shown in FIG. 7C. At this time, a passport icon 36F is displayed as the provider icon instead of the nonregistration icon 36D (step S46). By the display of this passport icon 36F, the user can know that registration of the terminal device 1 was already conducted. And the circuit is disconnected (step S48), and the processing returns to the step S16, and icon manipulation is waited.

If the nonpermission response is received as the response from the service provider (step S40), then a nonpermission message is displayed (step S50), the display is then returned to the telephone screen display (step S52), the processing proceeds to the step S48, and the circuit is disconnected. In this case, therefore, the nonregistration icon 36D remains displayed as the provider icon. Thereby, the user can know that the registration is not completed.

It is now assumed that the registration was completed as described above and icon manipulation is conducted on the telephone screen. If the icon manipulation is judged to be the manipulation of the provider icon (step S18), it is determined whether the provider registration completion flag is stored beforehand in the flash ROM 16 (step S20). This time, the provider registration completion flag is judged to be present. In this case, therefore, the circuit connection request (service request in this case) is transmitted to the specific provider (step S54), and the device kind code, ID, password, and telephone number of that terminal device 1 are transmitted (step S56). The password in this case may be one inputted by the user or one stored in the flash ROM 16.

In the server 2 of the provider, if the circuit connection request is not a registration request but a service request (step S100), then the device kind code, ID, password, and telephone number are received (step S114) and it is determined whether those received data are data of already registered user by referring to the user database 24-2 (step S116). If the data is impermissible received data from an unregistered user (step S118), then the processing proceeds to the above described step S112 and a nonpermission response is transmitted. On the other hand, if the user is a permissible registered user, a permission response is transmitted (step S120). Thereafter, a service menu corresponding to the device stored in the storage device 22 is selected (step S122), the service menu is transmitted (step S124), and the service is started.

In the side of the terminal device 1, if the response from the service provider is a permission response (step S58), then the service menu is received (step S60) and the received service menu screen is displayed as shown in FIG. 7D (step S62) in order to be able to be given various kinds of service.

If a nonpermission response is received, then a nonpermission message is displayed (step S64) and thereafter the processing is returned to the above described step S48 to disconnect the circuit.

If the provider registration completion flag is judged to be present at the step S12, then the passport icon 36F is displayed as the provider icon (step S66) and icon manipulation is waited (step S16).

In the portable terminal device 1 incorporating the telephone function according to the present first embodiment, the user thus needs only to input a desired password at the time on-line registration. The data required for the registration, such as the ID and the telephone number, are automatically added to the password by the terminal device 1 itself, and resultant data are transmitted to the service provider 2. As a result, the labor of the user registration procedure can be lightened.

A second embodiment will now be described.

The second embodiment is a system further simplifying the authentication.

When a provider is accessed by a personal computer or the like and provides predetermined service, the provider in general requests the user to input the user ID and the password in order to authenticate the user as a normal user. The server 2 installed in the provider of this system has a user database 24-2'. As for the terminal device 1, the user database 24-2' stores the telephone number of the terminal device 1 as the user name and the terminal number as the password as shown in FIG. 8.

The database is created by using data provided by a telephone company or the like.

An authentication method of the network system of this embodiment will be described by referring to FIG. 9.

Here, the authentication method will be described by taking the case where a user A is connected to the server 2 by using the terminal device 1 having the configuration of FIG. 2 and given data providing service of stock information or the like, as an example.

In order to connect to the server 2, the user A manipulates the input unit 15 and inputs the telephone number of the server 2. As this telephone number, the telephone number stored in the flash ROM 16 shown in the first embodiment may be used. In response to this manipulation, the CPU 11 calls the server 2 on the

phone (i.e., transmits a connection signal to the server 2) via the radio communication unit 17 (step A1).

The communication unit 25 of the server 2 receives the connection signal (i.e., connection request) transmitted from the terminal device 1 (step B1).

According to the connection signal supplied from the terminal device 1, the communication unit 25 conducts off-hook control, dial up control of the connection destination, and modem negotiation control between the terminal device 1 and the server 2 (step A2, step B2).

After the negotiation control has been finished, the CPU 21 sets a retry counter n taking the communication error into consideration to, for example, 3 (n = 3)(step B3). After setting the retry counter n, the CPU 21 transmits an input request signal requesting the terminal device 1 to input the user name and password for authentication to the terminal device 1 via the communication unit 25 (step B4).

The CPU 11 of the terminal device 1 receives the input request signal transmitted from the server 2 via the communication unit 17 (step A3), reads out the terminal information (i.e., the telephone number and the terminal number) stored in the flash ROM 16, and transmits the telephone number and the terminal number respectively as the user name and the password to the server 2 via the communication unit 17 (step A4).

The CPU 21 of the server 2 receives the telephone number and the terminal number transmitted respectively as the user name and the password from the terminal device 1 via the communication unit 25 (step B5) and store them in the RAM 22. The CPU 21 collates the user name (telephone number) and the password (terminal number) stored in the RAM 22 with the user name and the password stored in the database 24-2', and determines whether completely coinciding user name and password are present. If coincident data is present, then the CPU 21 authenticates the terminal device as a registered user, and permits the connection or the service provision (step B6). If coincident data is not present, the CPU 21 does not authenticate the other party of the connection and refuses the connection or the service provision (step B6).

If the terminal device 1 is authenticated at the step B6, the CPU 21 conducts processing for the connection and service provision, such as transmission of the selection menu of service stored in the storage unit 23 and capable of being provided by the server 2 to the terminal device 1 (step B7).

The CPU 11 of the terminal device 1 receives the selection menu transmitted from the server 2 via the communication unit 17, and displays the selection menu on the display unit 14. In addition, the CPU 11 accesses the server 2 according to the received selection menu, and enjoys the subsequent service (step A5). The server 2 provides service according to the request of the terminal device 1.

If it is determined at the step B6 that the terminal of the other party (terminal device 1) is not authenticated, the CPU 21 determines whether the retry counter n stored in the RAM 22 is 0 (n = 0) (step B8). If n is judged at the step B8 to be not equal to 0, then the retry counter n is decreased by one as represented by (n - 1) (step B9), the flow returns to the step B4 of the transmission of the input request signal, and the above described operation is conducted again.

If n is judged at the step B8 to be equal to 0, then the CPU 21 judges the received user name and password to be noncoincident with the terminal information of the database 24 of the server 2, i.e., judges the received user name and password not to be stored in the database 24 of the server 2, and conducts error processing, such as disconnection of the connected circuit (step A20).

In the case where one of the communication terminals 1-1 through 1-n, such as ordinary personal computers, request the server 2 to conduct connection, the communication terminal transmits the ordinary user name and password to the server 2. On the basis of this, the authentication processing of the step B6 is conducted.

In the above described embodiment, the telephone number and the terminal number are transmitted at the step A3 respectively as the user name and the password for authentication. Alternatively, the terminal number and the telephone number may be transmitted respectively as the user name and the password. In this case, the database 24 of the server 2 stores the terminal number as the user name and stores the telephone number as the password.

Furthermore, the telephone number (or the terminal number) may be transmitted as the password and the user name. In this case, the terminal information of the server 2 stores the telephone number (or the terminal number) as the user name and the password. As a result, the time required for the authentication can be shortened and the amount of transmission data can be suppressed.

In the foregoing description, the server 2 requests the terminal device to input the user name and the password at the step B4. Alternatively, the server 2 may judge the other party of communication, and request the ordinary user name and password in the case where the other party is an ordinary personal computer or the like, or request the telephone number and the terminal number in the case where the other party of communication is a PDA or the like having a unique telephone number or the like and a telephone function.

In this case, a flag besides the data of the telephone number or the like is prepared in the database 24 of the server 2 as information of a user who contracted with (registered in) the provider as shown in FIG. 10. The flag identifies whether the communication terminal 1-1 through 1-n used by the user is a device having a telephone function, such as a PDA, or a device having no unique telephone number, such as a personal com-

puter.

Upon being informed of the telephone number of the transmission source by an exchange or the like at the time of call incoming (terminating call), the server 2 determines whether the flag is set in the informed telephone number by referring to the database 24. If the flag is set beforehand to "1", i.e., the other party of the communication is a PDA having a telephone function, then the server 2 requests the terminal to transmit the telephone number and the terminal number as the authentication information. If the flag is set beforehand to "0", i.e., the other party of the communication is an ordinary personal computer or the like, then the server 2 requests the user name (including the user ID) and the password.

By using such a configuration, authentication conformed to the property of the other party of the communication becomes possible.

In some cases, a fixed form is demanded for the user name and the password requested by the service program on the server 2, and the telephone number and the terminal number cannot be used as they are as the user name and the password. In such a case, a kind of agent program may be located on the server 2. After conducting the authentication processing by using the telephone number and the terminal number, the agent program provides the user name and the password in a predetermined form to the service program.

Processing in this case will now be described by referring to FIG. 11.

First of all, the agent program and data for authentication are set beforehand in the storage unit 23 of the server 2. The data for authentication includes the telephone number and the terminal number of a registered user, and the user name and the password set beforehand for the service program as shown in FIG. 11.

Upon being called by one of the communication terminals 1-1 through 1-n, the CPU 21 of the server 2 starts the agent program on the storage unit 23.
The agent program conducts the processing of the steps B1 through B6, and conducts the authentication of the terminal of the other party. Upon completion of the authentication of the terminal of the other party, the agent program provides the service program with the user name and the password registered beforehand in association with the telephone number or the like as shown in FIG. 11.

The service program confirms that the provided user name and password are registered validly beforehand and starts provision of the service to the terminal device being connected.

Alternatively, the list shown in FIG. 11 may be registered beforehand in the database 24 of the server 2. In this case, the agent program is started only when the terminal of the other party is judged to be a specific device kind such as a PDA having a telephone function. Otherwise, the authentication processing shown in FIG. 9 is conducted.

In the foregoing description, the server 2 requests the terminal device to transmit the user name and the password in Step B4. However, in the case where the exchange office or the like informs of the telephone number of the other party of communication at the timing of call incoming, that telephone number may used as it is for authentication.

Claims

1. A communication processing device conducting data communication with a communication service providing device connected via a communication circuit, said communication processing device characterized by comprising:

   a first memory for storing a unique information assigned beforehand;
   input guide means for causing a user to input a password for registering in said communication service providing device in response to specification of registration processing execution of its own communication processing device with respect to said communication service providing device; and
   transmission means for transmitting said password inputted by the user according to said input guide means and said unique information stored in said first memory to said communication providing device,
   wherein registration of its own communication processing device with respect to said communication service providing device is conducted by using said unique information and password.

2. The communication processing device according to claim 1, characterized by further comprising:

   commanding means for commanding connection to said communication service providing device;
   a second memory for storing information indicating whether its own processing device has been registered in said communication service providing device; and
   control means for judging contents of said second memory in response to a connection command to said specific communication service providing device given by said commanding means, said control means causing a service request connection to be executed if already registered and causing registration processing to be executed if not registered.

3. The communication processing device according to claim 2, characterized in that said commanding means comprises means for displaying an identifier

as a menu item for connection to said communication service providing device, said displaying means displays the identifier in a mode differing according to contents of said second memory.

4. The communication processing device according to claim 3, characterized by further comprising a third memory storing beforehand a telephone number for connection to said communication service providing device.

5. An authentication system in a network system including a server and terminal devices, the server authenticating a terminal device based on data transmitted by the terminal device, the server providing an authenticated terminal device with service,

said server comprising:

terminal information storing means for storing terminal information including a terminal code and a telephone number belonging to each of said terminal devices;
receiving means for receiving a connection request and terminal information of a terminal device transmitted from said terminal devices; and
authentication means for collating said terminal information transmitted from said terminal device with said terminal information stored in said terminal information storing means, and for authenticating said terminal device and permitting the connection when substantial coincidence is found, and

each of said terminal devices comprising:

storing means for storing a terminal code of said terminal device and a telephone number assigned to said terminal device as terminal information; and
transmitting means for transmitting a connection request and said terminal information stored in said storing means to said server.

6. The authentication system according to claim 5, characterized in that said authentication means conducts authentication by using user identification information and a password, and said authentication means comprises means handling one of a terminal number and a telephone number received from said terminal device as the user identification information and the other as the password.

7. A terminal device having a telephone function, said terminal device being connected to a server via a network in order to be given information providing service, said terminal device characterized by comprising:

storing means for storing information unique to said terminal device and a telephone number assigned to said terminal device; and
transmission means for transmitting the information unique to said terminal device and the telephone number stored in said storing means to said server as authentication data when said terminal device is connected to said server.

8. The terminal device according to claim 7, characterized by further comprising connection telephone number storing means for storing beforehand a telephone number of a predetermined network service provider having said server.

9. The terminal device according to claim 7, characterized in that said transmission means comprises means for transmitting one of the information unique to the terminal and the telephone number stored in said storing means as user identification information and the other as the password to said server, when said server requests said terminal device to input the user identification information and the password as authentication information.

10. The terminal device according to claim 7, characterized in that said transmission means comprises means for transmitting one of the information unique to the terminal and the telephone number stored in said storing means as user identification information and information inputted by a user as the password to said server, when said server requests said terminal device to input the user identification information and the password as authentication information.

11. A server for providing terminal devices having a telephone function connected to said server via a public telephone circuit with communication service, said server characterized by comprising:

terminal information storing means for storing terminal information including at least one of information unique to a terminal and a telephone number of each of said terminal devices;
receiving means for receiving the information unique to a terminal and/or the telephone number of the terminal device when the terminal device has requested connection; and
authentication means for collating the information unique to the terminal and/or the telephone number received by said receiving means with said terminal information stored in said terminal information storing means, and for deter-

mining whether said terminal device should be connected to said server.

12. The server according to claim 11, characterized in that said authentication means conducts authentication by using user identification information and a password, and said authentication means comprises means handling one of a terminal number and a telephone number received from said terminal device as the user identification information and the other as the password.

FIG.1

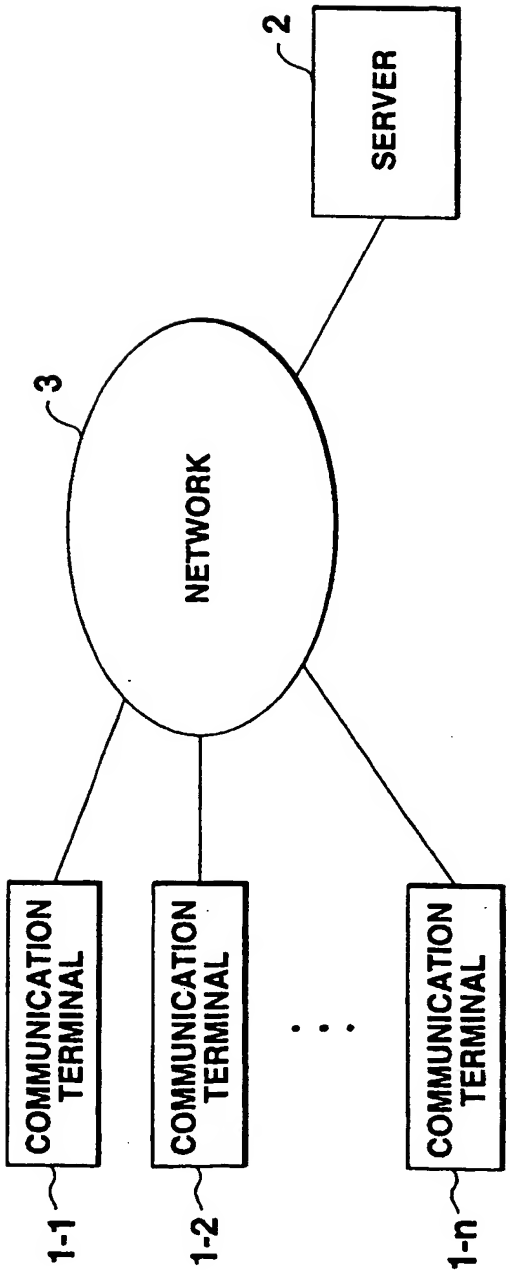

2
SERVER
3
NETWORK
COMMUNICATION TERMINAL
COMMUNICATION TERMINAL
COMMUNICATION TERMINAL
1-1
1-2
1-n

FIG.2

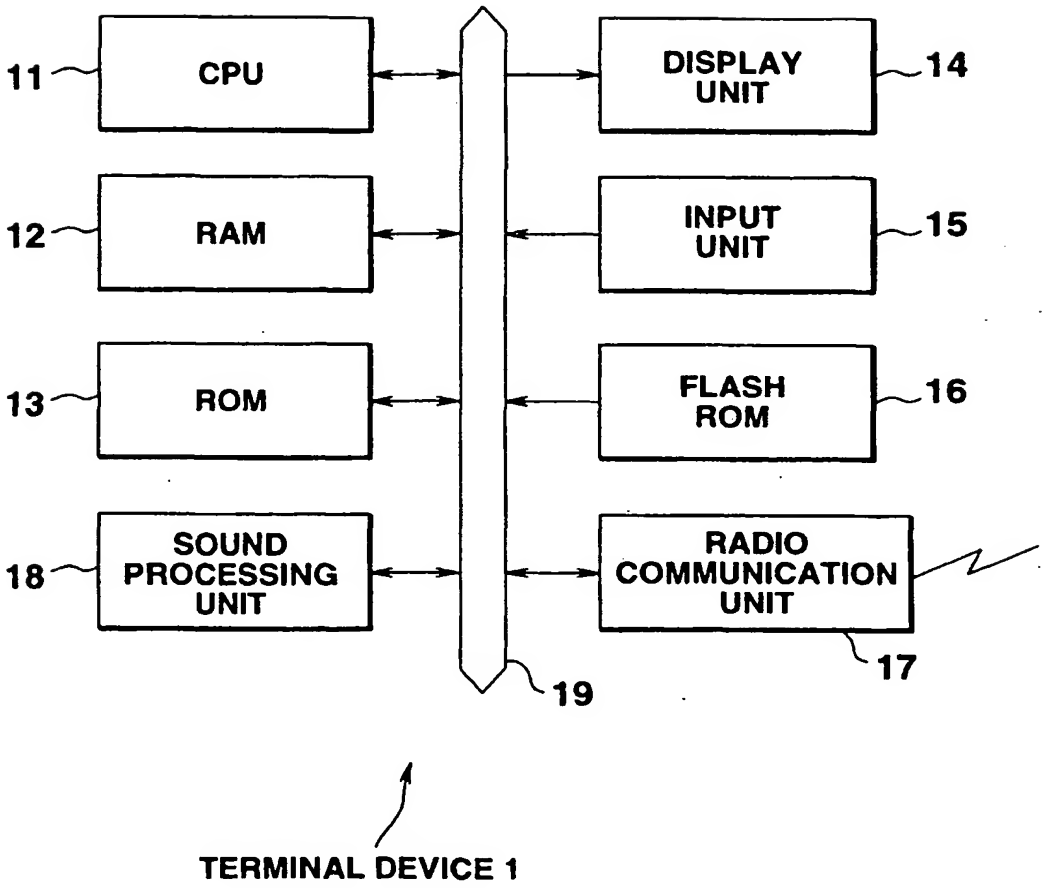

11
CPU
12
RAM
13
ROM
18
SOUND PROCESSING UNIT
DISPLAY UNIT
14
INPUT UNIT
15
FLASH ROM
16
RADIO COMMUNICATION UNIT
17
19
TERMINAL DEVICE 1

FIG.3

TELEPHONE NUMBER	01-2345-6789
DEVICE KIND CODE	CX001
TERMINAL NUMBER (ID)	XX-00-X-000
PROVIDER TELEPHONE NUMBER	03-9876-5432
REGISTRATION COMPLETION FLAG	
(PASSWORD)	

FIG.4

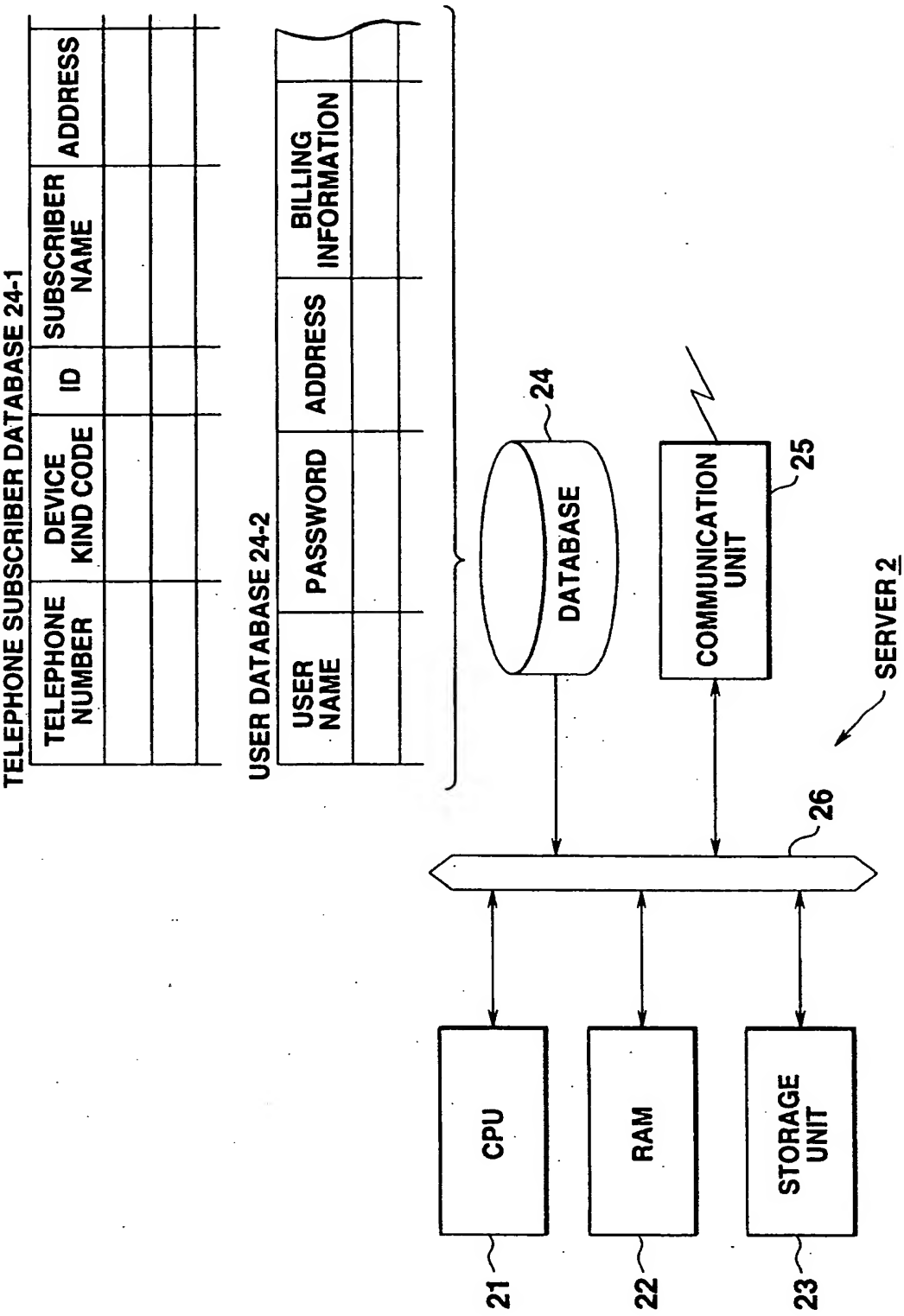

TELEPHONE SUBSCRIBER DATABASE 24-1
TELEPHONE NUMBER
DEVICE KIND CODE
ID
SUBSCRIBER NAME
ADDRESS
USER DATABASE 24-2
USER NAME
PASSWORD
ADDRESS
BILLING INFORMATION
24
DATABASE
COMMUNICATION UNIT
25
SERVER 2
26
CPU
RAM
STORAGE UNIT
21
22
23

FIG.5A

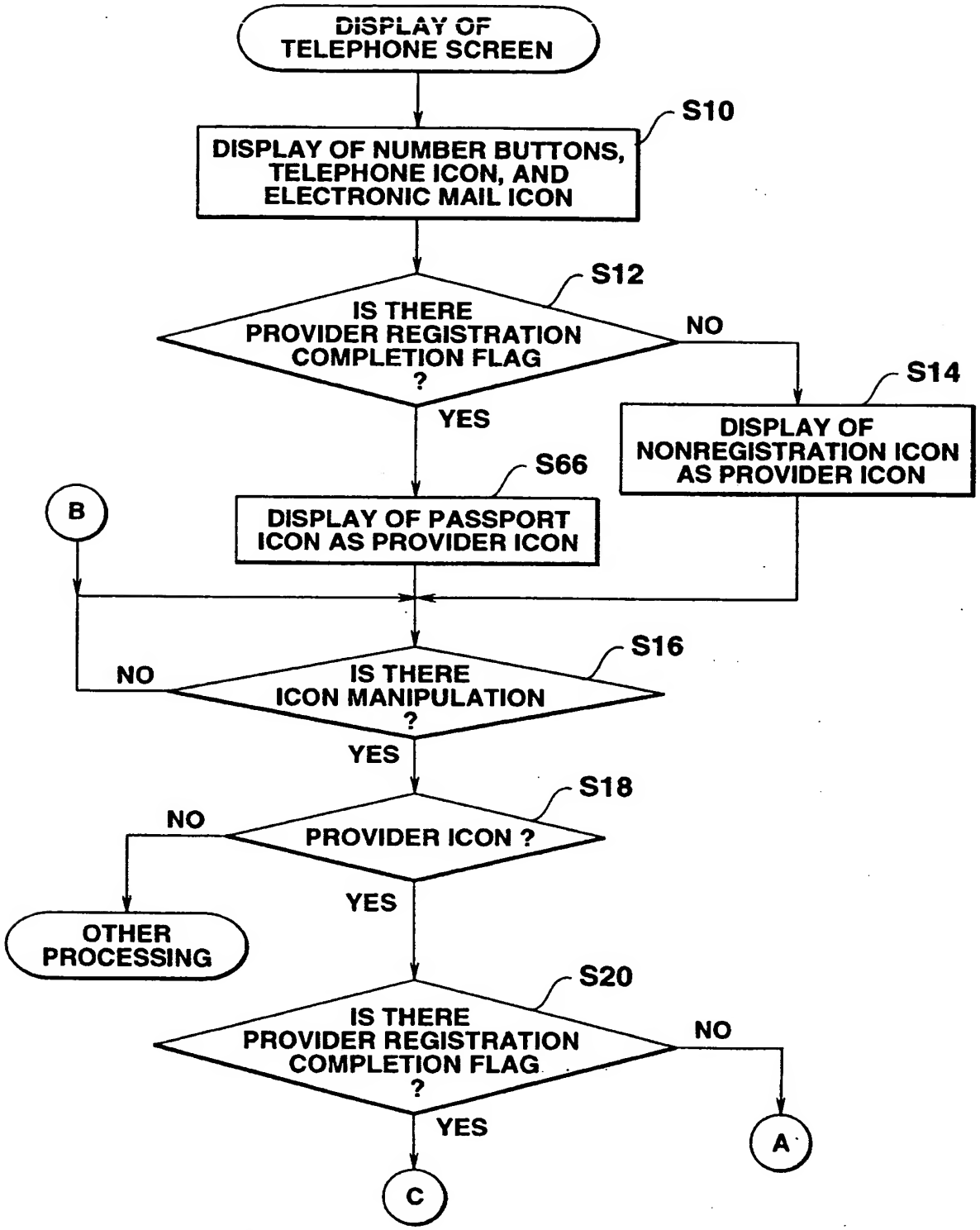

DISPLAY OF TELEPHONE SCREEN
S10
DISPLAY OF NUMBER BUTTONS, TELEPHONE ICON, AND ELECTRONIC MAIL ICON
S12
IS THERE PROVIDER REGISTRATION COMPLETION FLAG ?
NO
YES
S14
DISPLAY OF NONREGISTRATION ICON AS PROVIDER ICON
S66
DISPLAY OF PASSPORT ICON AS PROVIDER ICON
B
S16
NO
IS THERE ICON MANIPULATION ?
YES
S18
NO
PROVIDER ICON ?
YES
OTHER PROCESSING
S20
IS THERE PROVIDER REGISTRATION COMPLETION FLAG ?
NO
YES
A
C

FIG.5B

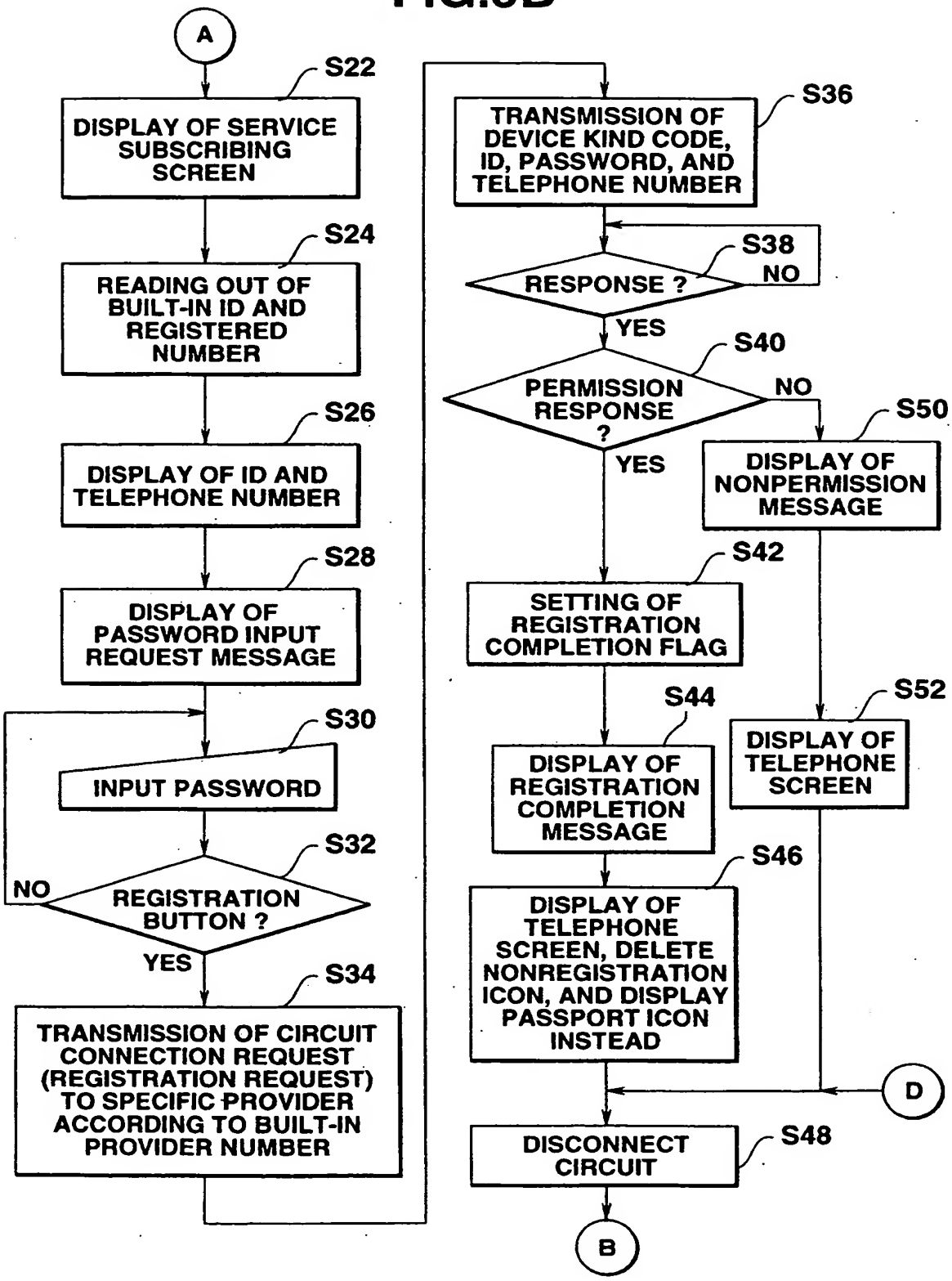

A
S22
DISPLAY OF SERVICE SUBSCRIBING SCREEN
S24
READING OUT OF BUILT-IN ID AND REGISTERED NUMBER
S26
DISPLAY OF ID AND TELEPHONE NUMBER
S28
DISPLAY OF PASSWORD INPUT REQUEST MESSAGE
S30
INPUT PASSWORD
S32
NO
REGISTRATION BUTTON ?
YES
S34
TRANSMISSION OF CIRCUIT CONNECTION REQUEST (REGISTRATION REQUEST) TO SPECIFIC PROVIDER ACCORDING TO BUILT-IN PROVIDER NUMBER
S36
TRANSMISSION OF DEVICE KIND CODE, ID, PASSWORD, AND TELEPHONE NUMBER
S38
NO
RESPONSE ?
YES
S40
PERMISSION RESPONSE ?
NO
YES
S50
DISPLAY OF NONPERMISSION MESSAGE
S42
SETTING OF REGISTRATION COMPLETION FLAG
S44
DISPLAY OF REGISTRATION COMPLETION MESSAGE
S52
DISPLAY OF TELEPHONE SCREEN
S46
DISPLAY OF TELEPHONE SCREEN, DELETE NONREGISTRATION ICON, AND DISPLAY PASSPORT ICON INSTEAD
D
S48
DISCONNECT CIRCUIT
B

FIG.5C

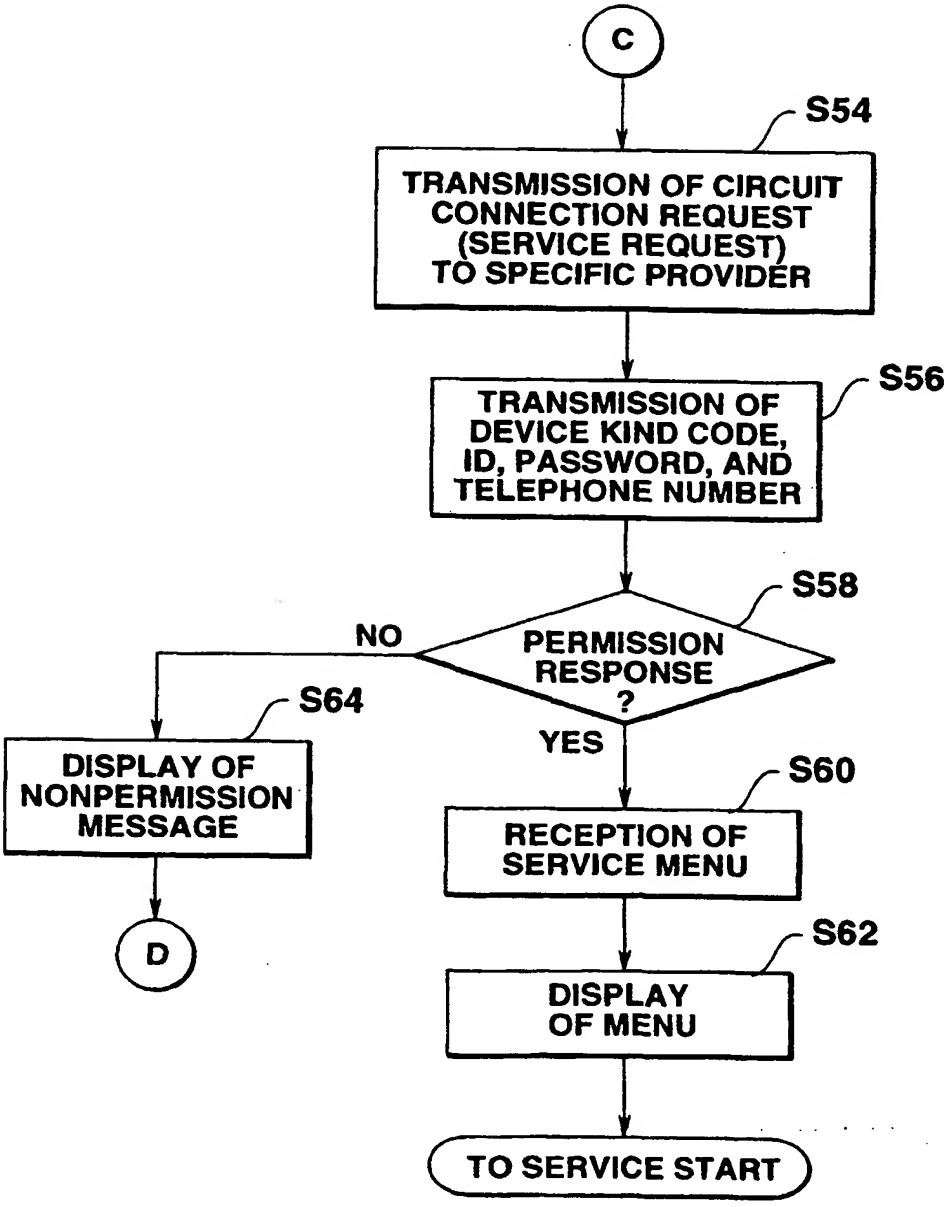

C
S54
TRANSMISSION OF CIRCUIT CONNECTION REQUEST (SERVICE REQUEST) TO SPECIFIC PROVIDER
S56
TRANSMISSION OF DEVICE KIND CODE, ID, PASSWORD, AND TELEPHONE NUMBER
S58
PERMISSION RESPONSE ?
NO
YES
S64
DISPLAY OF NONPERMISSION MESSAGE
D
S60
RECEPTION OF SERVICE MENU
S62
DISPLAY OF MENU
TO SERVICE START

FIG.6

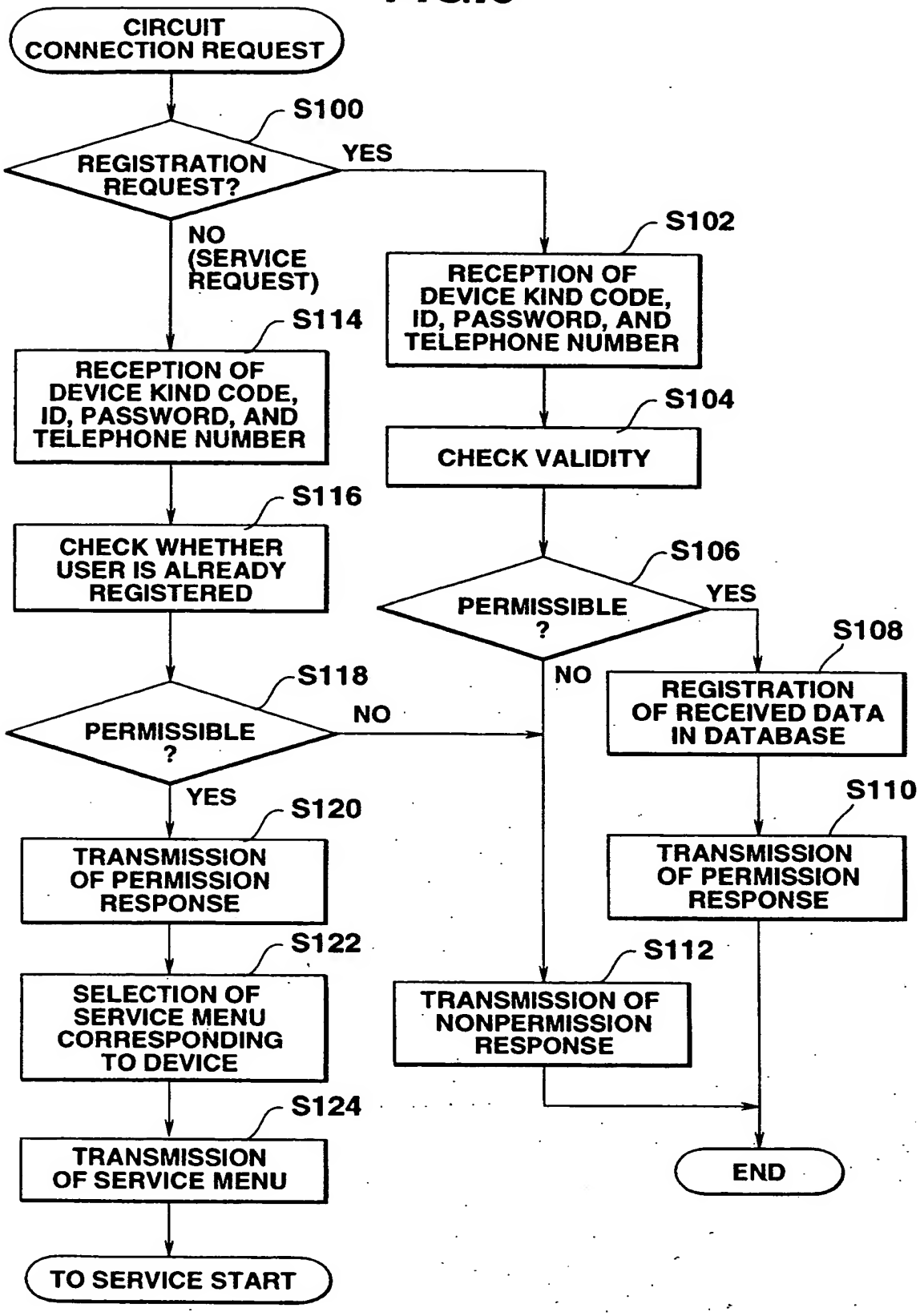

CIRCUIT CONNECTION REQUEST
S100
REGISTRATION REQUEST?
YES
NO (SERVICE REQUEST)
S102
RECEPTION OF DEVICE KIND CODE, ID, PASSWORD, AND TELEPHONE NUMBER
S104
CHECK VALIDITY
S106
PERMISSIBLE ?
YES
NO
S108
REGISTRATION OF RECEIVED DATA IN DATABASE
S110
TRANSMISSION OF PERMISSION RESPONSE
S112
TRANSMISSION OF NONPERMISSION RESPONSE
END
S114
RECEPTION OF DEVICE KIND CODE, ID, PASSWORD, AND TELEPHONE NUMBER
S116
CHECK WHETHER USER IS ALREADY REGISTERED
S118
PERMISSIBLE ?
NO
YES
S120
TRANSMISSION OF PERMISSION RESPONSE
S122
SELECTION OF SERVICE MENU CORRESPONDING TO DEVICE
S124
TRANSMISSION OF SERVICE MENU
TO SERVICE START

FIG.7A

TELEPHONE SCREEN
(WHEN NOT YET REGISTERED)

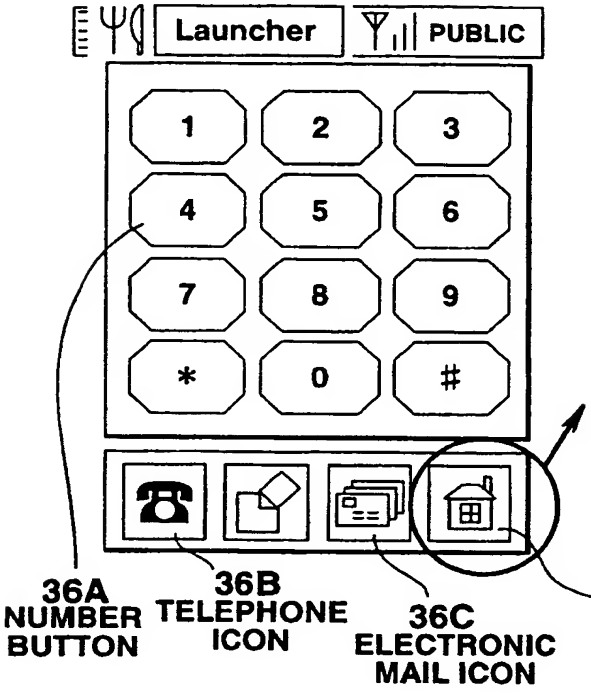


FIG.7B

SERVICE SUBSCRIBING SCREEN

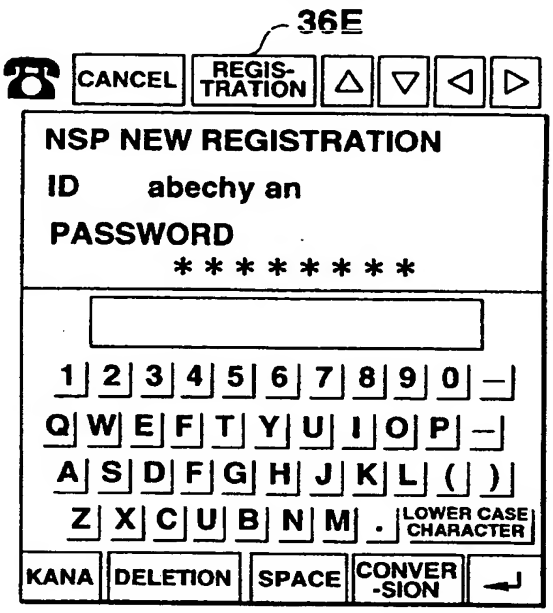


FIG.7C

TELEPHONE SCREEN
(AFTER REGISTRATION)

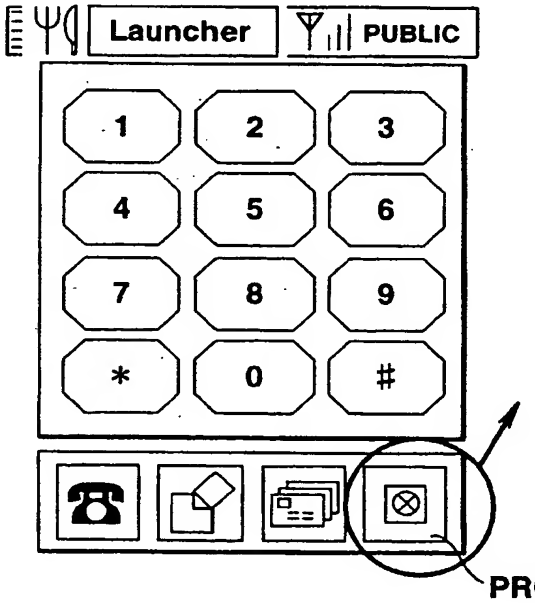


FIG.7D

SERVICE MENU SCREEN

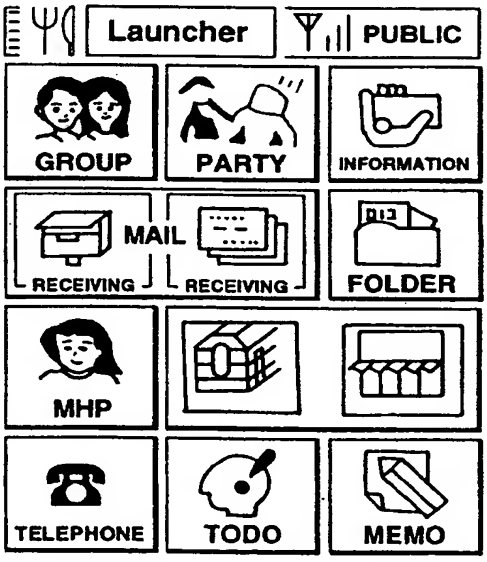


FIG.8

USER NAME	PASSWORD	USER INFORMATION
01-2345-6789	○○-○○-○-○○○	○○××
01-9999-8888	○○-××-○-×××	△△□□
⋮	⋮	⋮

FIG.9

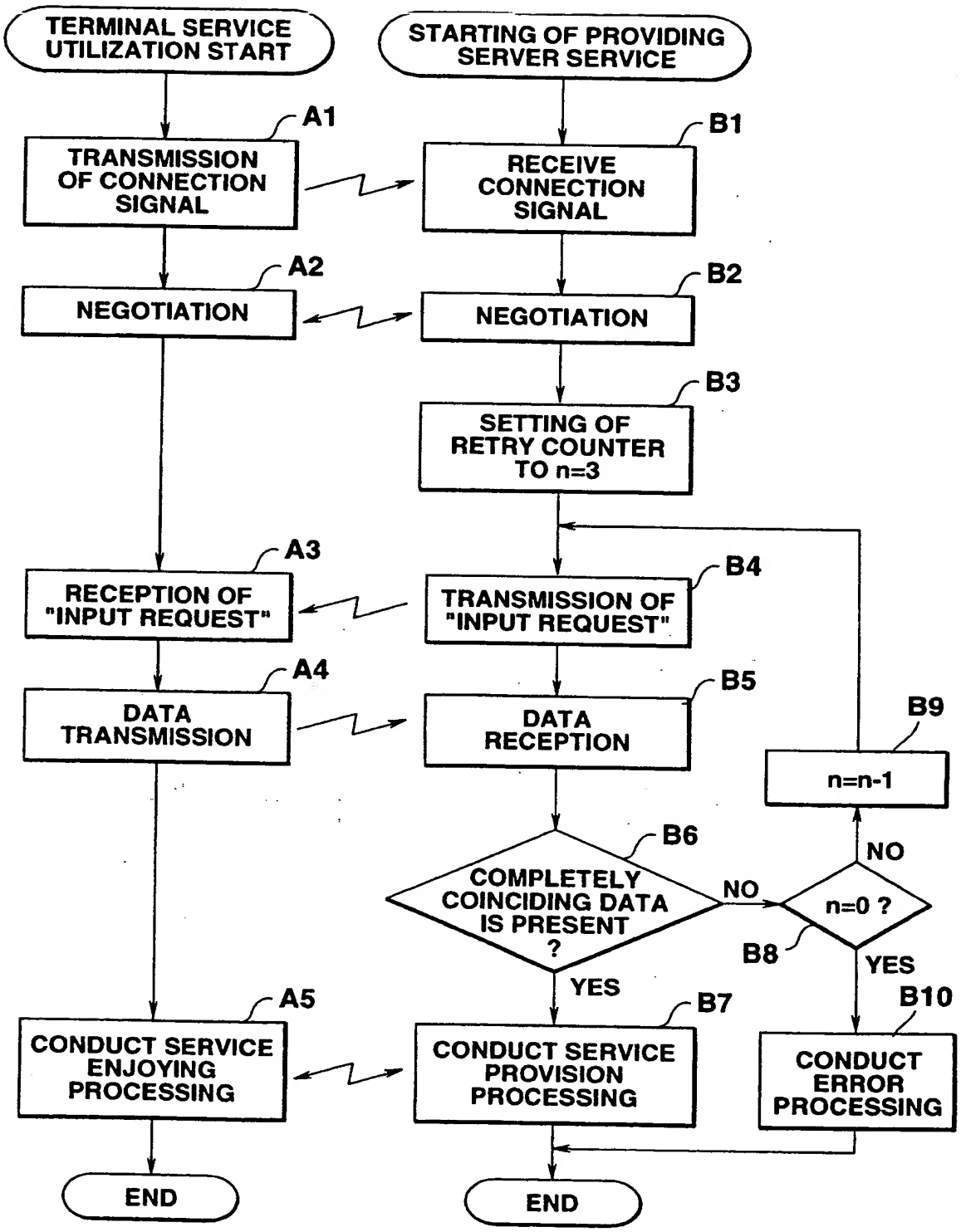

TERMINAL SERVICE UTILIZATION START
STARTING OF PROVIDING SERVER SERVICE
A1
TRANSMISSION OF CONNECTION SIGNAL
B1
RECEIVE CONNECTION SIGNAL
A2
NEGOTIATION
B2
NEGOTIATION
B3
SETTING OF RETRY COUNTER TO n=3
A3
RECEPTION OF "INPUT REQUEST"
B4
TRANSMISSION OF "INPUT REQUEST"
A4
DATA TRANSMISSION
B5
DATA RECEPTION
B9
n=n-1
B6
COMPLETELY COINCIDING DATA IS PRESENT ?
NO
n=0 ?
NO
B8
YES
YES
A5
CONDUCT SERVICE ENJOYING PROCESSING
B7
CONDUCT SERVICE PROVISION PROCESSING
B10
CONDUCT ERROR PROCESSING
END
END

FIG.10

TELEPHONE NUMBER	FLAG	DEVICE KIND	USER NAME	PASSWORD	USER INFORMATION
030-1234-5678	1	DATA PHS	030-1234-5678	01223456	CHIYODA-KU...
03-4567-8910	0	PDA	××××	1334567	SUGINAMI-KU...
060-8910-1112	1	PDA WITH TELEPHONE FUNCTION	044-8910-1112	3333333	KAWASAKI CITY...
⋮	⋮	⋮	⋮	⋮	⋮

EP 0 862 104 A2

FIG.11

TELEPHONE NUMBER	PASSWORD	USER NAME	PASSWORD
030-1234-4567	12345678	PAD1212	jxbu333
06-1111-2222	44466677	AXZ3434	uuuki572
-------	-------	-------	-------

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 862 104 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
20.12.2000 Bulletin 2000/51

(43) Date of publication A2:
02.09.1998 Bulletin 1998/36

(21) Application number: **98103380.6**

(22) Date of filing: **26.02.1998**

(51) Int. Cl.[7]: **G06F 1/00**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **28.02.1997 JP 4603897**
16.12.1997 JP 36333597

(71) Applicant:
Casio Computer Co., Ltd.
Shibuya-ku, Tokyo 151-8543 (JP)

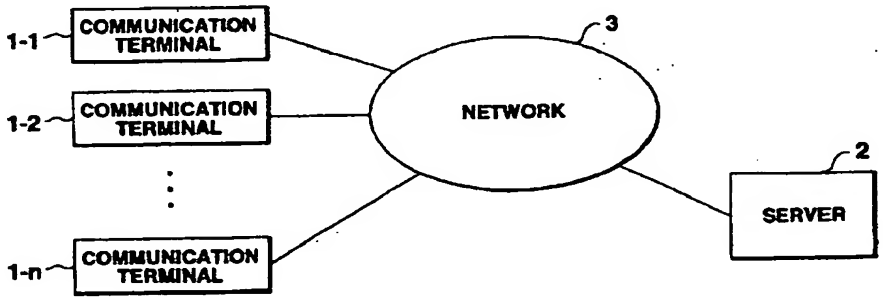
(72) Inventors:
- **Moriya, Koji,**
  c/o Casio Computer Co., Ltd.
  Hamura-shi, Tokyo 205-8555 (JP)
- **Morikawa, Shigenori,**
  c/o Casio Computer Co., Ltd.
  Hamura-shi, Tokyo 205-8555 (JP)

(74) Representative:
Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) Authentication system using network

(57) A communication terminal (1) stores an assigned telephone number and a number unique to the terminal. When on-line registration is to be conducted with respect to a server (2), a registration screen is automatically created. On the registration screen, predetermined information is already described as entry matters required for registration by using the above described numbers. By inputting a password to this screen, the user can complete on-line registration simply. When the server (2) provides service, the server requests the user to input the user name and the password. As for the communication terminal (1), the server has beforehand the telephone number, information unique to the terminal, and the like in the database. In response to a communication request from the communication terminal (1), the server (2) conducts authentication by using the telephone number as the user name and the terminal number as the password.

FIG.1



EP 0 862 104 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 10 3380

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	WO 95 20864 A (HJERN MAGNUS ;OLANDERS PETER (SE); TELIA AB (SE)) 3 August 1995 (1995-08-03) * abstract * * page 1, line 31 - page 2, line 5 * * page 5, line 4 - page 8, line 17 *	1,2,5,7, 11,12	G06F1/00
A		2-4,6, 8-10	
A	EP 0 497 203 A (BELLSOUTH CORP) 5 August 1992 (1992-08-05) * abstract; figure 4 * * page 2, line 41 - line 57 * * page 5, line 22 - line 37 * * claims 1-65 *	1-12	
A	EP 0 745 924 A (AT & T CORP) 4 December 1996 (1996-12-04) * abstract; figure 1 * * column 1, line 21 - line 37 * * column 5, line 31 - column 6, line 24 *	1-12	TECHNICAL FIELDS SEARCHED (Int.Cl.6)
A	WO 95 15066 A (ERICSSON TELEFON AB L M) 1 June 1995 (1995-06-01)		G06F H04M H04L H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	31 October 2000	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 10 3380

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

31-10-2000.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9520864 A	03-08-1995	EP 0741952 A	13-11-1996
		SE 9400265 A	29-07-1995
		US 5812948 A	22-09-1998
EP 0497203 A	05-08-1992	US 5610973 A	11-03-1997
		AT 168514 T	15-08-1998
		AU 661838 B	10-08-1995
		AU 1321792 A	27-08-1992
		BR 9205718 A	19-04-1994
		DE 69226210 D	20-08-1998
		DE 69226210 T	25-02-1999
		FI 933371 A	21-09-1993
		IE 80947 B	14-07-1999
		MX 9200343 A	31-03-1994
		NO 932712 A	27-09-1993
		NZ 241430 A	27-06-1994
		WO 9213416 A	06-08-1992
		US 6108537 A	22-08-2000
		US 5588042 A	24-12-1996
EP 0745924 A	04-12-1996	US 5721780 A	24-02-1998
		CA 2172566 A	01-12-1996
		JP 8340331 A	24-12-1996
WO 9515066 A	01-06-1995	AU 677482 B	24-04-1997
		AU 1126095 A	13-06-1995
		BR 9406070 A	06-02-1996
		CA 2153873 A	01-06-1995
		CN 1117338 A	21-02-1996
		SE 9502657 A	07-09-1995
		US 5557676 A	17-09-1996

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82